What Is a DDoS Attack?

Distributed-denial-of-service (DDoS) attacks are sophisticated attacks designed to flood the network with superfluous traffic. A DDoS attack results in either degraded network performance or outright service outage of critical infrastructure.

Cisco Secure DDoS | Read At-a-Glance

How long does a DDoS attack last?

The length of a DDoS attack varies. Attacks like the Ping of Death can be short. The Slowloris attack takes longer to develop. According to a Radware report, 33 percent of DDoS attacks last an hour; 60 percent last less than a full day; and 15 percent last as long as a month.

Why would someone carry out a DDoS attack?

There are many motives for DDoS attacks, ranging from disruption of services to espionage and cyber warfare. Some common motives include:

- Make a political statement (hacktivism)
- Disrupt communications and essential services
- Gain a competitive advantage
- Achieve financial gain through extortion, theft, etc.
- Inflict brand/reputational damage
- Steal or destroy confidential information or intellectual property
- Launch a ransomware attack
- Wage cyber warfare

Which industries are being targeted and why?

While DDoS attacks are a threat to all businesses and all industries, DDoS attacks most often target the following:

- **Online gaming and gambling**: To win a competitive advantage or financial gain.
- **Service providers**: To commit data theft, eavesdrop, disrupt essential services, or inflict reputational damage.
- **Cloud services (AWS, Azure, etc.)**: To commit data theft, eavesdrop, disrupt essential services, or inflict reputational damage.
- **Governments**: To steal intellectual property, disrupt operations, eavesdrop, commit espionage, or gain a competitive advantage.
- **Financial services**: To achieve financial gain, inflict reputational damage, access confidential data, or cause disruption.
- **Online retailers**: To disrupt operations, gain a competitive advantage, inflict reputational damage, or steal intellectual property.

Five Steps to Protecting Your Organization from a DDoS Attack

Protecting your business

Defending against DDoS attacks is a crucial part of securing your network. You must deploy a complete and holistic IT approach that uses components capable of seamlessly working together in an integrated platform.

Learn about Cisco SecureX >

Latest trends in DDoS attacks

Denial-of-service attacks were originally used by hacktivists to disrupt network access. Today's DDoS attacks are more sophisticated and far more damaging, and the number of DDoS attacks is expected to double to 15.4 million by 2023. The following trends have resulted in escalating damage.

Botnets

IoT botnets are being harnessed to launch massive, volumetric DDoS attacks that can quickly overwhelm networks.

Application layer

Sophisticated application-layer (L7) attacks exhaust server resources and bring services to a standstill. L7 has become the attack vector of choice.

Encryption

An estimated 90 percent of internet traffic is now encrypted, and attackers are using encrypted traffic to launch a flood of powerful SSL DDoS attacks.

Volume

Primarily due to botnets, the volume of DDoS attacks continues to grow. The Dyn DDoS attack in October 2016 was 1.2 Tbps. Just over three years later, AWS observed a 2.3 Tbps UDP reflection attack that is believed to be the largest DDoS attack in history.

Tools

Another troubling trend is the widespread availability of tools that help malicious actors launch devastating DDoS attacks easily, quickly, and inexpensively. These include tools to:

- Leverage DDoS-as-a-service
- Buy/rent a turnkey, ready-to-go botnet
- Use widely available public information to build a DDoS attack
- Hire a contractor to build and execute a DDoS attack

Learn about DDoS-for-hire >

Learn more

Cisco Secure DDoS Protection

Cisco Secure DDoS Protection At-a-Glance

Five Steps to Protecting Your Organization from a DDoS Attack

Related Cisco technologies

Cisco Firepower 4100 Series firewalls

Cisco Firepower 9000 Series next-generation firewalls

Cisco Firepower 9300 Series appliances with Radware technology

Related security topics

What Is Vulnerability Management?

Common Cyber Attacks

Network Security Checklist

What Is a VPN?

What Is Phishing?

What Is Network Security?

Disaster Recovery Plan

Connect with us

Free trials for Security

By continuing to use our website, you acknowledge the use of cookies.

Privacy Statement > Change Settings >